VA Software Assurance

Office of Information Security

Secure Coding Tips

Tip: Errors Encountered During Fortify Scans May Affect Results

This week's Secure Coding Tip is about errors reported during scans of source code using the HP Fortify Static Code Analyzer (SCA) software. Scanning source code to perform code review is an authorization requirement included in the Technical / Testing Requirements of the OCS Accreditation Requirements Guide / SOP [1] , and enforced as part of the ATO issuance process.[2]

One of the top 10 issues[3] encountered by VA application developers using the HP Fortify SCA software are errors reported during the scan[4]. While some scan errors are benign warnings, most affect the results reported by Fortify. All scanning errors which may affect the results must be resolved according to the OIS Secure Code Review Standard Operating Procedures (SOP)[5] to ensure the most accurate set of results.

There are several steps you should take to try to resolve the issue. **Read more…**

[1] "Accreditation Requirements Guide / Standard Operating Procedures", Office of Cyber Security (OCS) Assessment and Authorization intranet site.

[2] "Accreditation Requirements Expectation Memorandum" (Section 2.a.ii "Code Review"), VA Chief Information Security Officer (CISO) Stanley F. Lowe, March 19, 2014.

[3] **VA Top 10 Fortify Scan Issues For 2015 (Q1)**

[4] VA Top 10 Fortify Scan Issues For 2015 (Q1), **S1: Errors during scan**

[5] **OIS Secure Code Review SOP**

More Information

For more information about the VA Software Assurance Program Office, please visit our website **here**.